What Is Claimed Is:

1. A method implemented in a computer system for enabling a sender to send documents, said method comprising:

enabling said sender generate an electronic file containing an user input;

generating a first digital signature based on a first data containing said user input;

generating a second digital signature based on second data containing said user input, wherein said second data is different from said first data; and

sending said first digital signature and said second digital signature to a receiver system,

wherein said receiver system verifies the integrity of said user input by using one of both of said first digital signature and said second digital signature.

2. The method of claim 1, wherein said first data comprises said user input only, and wherein said second data comprises an electronic file containing said user input.

3. The method of claim 2, wherein said second data further comprises a user signature, and said electronic file comprises an electronic document.

4. The method of claim 3, wherein said first digital signature and second digital signature are generated using the same hash operation.

5. The method of claim 3, wherein said user signature comprises a biometric signature.

6. The method of claim 5, wherein said biometric signature comprises a handwritten signature of said sender.

7. The method of claim 3, further comprising encrypting said electronic file, said first

and second digital signatures and said user signature to generate encrypted data, wherein said encrypted data is examined by said receiver system to verify the integrity of said user input.

8. The method of claim 7, wherein said encrypted data is sent to said receiver system on either Internet or a dial-up connection.

9. The method of claim 3, further comprising generating a plurality of content digital signatures, wherein each of said plurality of content digital signatures is based on user input contained in a portion of said electronic document.

10. The method of claim 9, further comprising storing a control section associated with said electronic document, wherein said control section includes audit information associated with at least one of said plurality of content digital signatures.

11. The method of claim 9, further comprising storing a control section associated with said electronic document, wherein said control section includes a rule associated with at least one of said plurality of content digital signatures, wherein said rule specifies an action either permitted or prohibited against the corresponding section.

12. The method of claim 11, wherein said action comprises one of whether the corresponding section can be printed or not, and whether the corresponding section can be modified or not.

13. A method implemented in a computer system for enabling a receiver to receive electronic documents, said method comprising:

receiving a first data containing a user input and at least a first digital signature and a second digital signature, wherein said first digital signature and said second digital signature are generated based on data containing said user input; and

examining said first signature and/or second signature to determine the integrity of said user input.

14. The method of claim 13, wherein said first data further contains a user signature and said user input is contained in an electronic document.

15. The method of claim 14, wherein said first signature is generated based on said user input only and wherein said second signature is generated based on said electronic document.

16. A method of generating electronic documents, said method comprising:

enabling a user to generate an electronic document comprising a plurality of portions;

enabling said user to specify a rule associated with each of said plurality of portions;

generating a digital signature associated with each of said plurality of portions;

including a control section in said electronic document, wherein said control section specifies said rules associated with the corresponding portions.

17. A computer system for enabling a sender to send documents, said computer system comprising:

means for enabling said sender generate an electronic file containing an user input;

means for generating a first digital signature based on a first data containing said user input;

means for generating a second digital signature based on second data containing said user input, wherein said second data is different from said first data; and

means for sending said first digital signature and said second digital signature to a receiver system,

wherein said receiver system verifies the integrity of said user input by using one of both of said first digital signature and said second digital signature.

18. A computer system for enabling a receiver to receive electronic documents, said computer system comprising:

means for receiving a first data containing a user input and at least a first digital signature and a second digital signature, wherein said first digital signature and said second digital signature are generated based on data containing said user input; and

means for examining said first signature and/or second signature to determine the integrity of said user input.

19. A computer readable medium carrying one or more sequences of instructions for causing for enabling a sender to send documents, wherein execution of said one or more sequences of instructions by one or more processors contained in said device causes said one or more processors to perform the actions of:

enabling said sender generate an electronic file containing an user input;

generating a first digital signature based on a first data containing said user input;

generating a second digital signature based on second data containing said user input, wherein said second data is different from said first data; and

sending said first digital signature and said second digital signature to a receiver system,

wherein said receiver system verifies the integrity of said user input by using one of both of said first digital signature and said second digital signature.